UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA
Plaintiff,

v. **Case No. 13-CR-120**

PAUL CASE
Defendant.

DECISION AND ORDER

The government charged defendant Paul Case with distribution and possession of child pornography. Pursuant to Franks v. Delaware, 438 U.S. 154 (1978), defendant moved to suppress evidence obtained pursuant to a search warrant, arguing that the agent who applied for the warrant misled the issuing magistrate judge by failing to disclose the FBI's use of an automated computer program to discover child pornography files on defendant's computer available for download through a peer-to-peer ("P2P") file sharing network. Defendant further claimed that the program may have infiltrated non-shared, private portions of his computer, in violation of the Fourth Amendment. The magistrate judge handling pre-trial proceedings in this case denied the request for a Franks hearing and recommended that the motion to suppress be denied. Defendant objects. I review the recommendation de novo. Fed. R. Crim. P. 59(b).

I. FRANKS FRAMEWORK

Search warrants enjoy a presumption of validity. See Franks, 438 U.S. at 171; United States v. Walker, 25 F.3d 540, 544 (7th Cir. 1994). A defendant is entitled to an evidentiary hearing to examine the sufficiency of a search warrant only if he makes a "substantial preliminary showing" that the warrant application contained a materially false statement made

by law enforcement with deliberate or reckless disregard for the truth and that the false statement was necessary for the finding of probable cause. United States v. Williams, 718 F.3d 644, 649 (7th Cir. 2013) (citing Franks, 438 U.S. at 155-56). A defendant may also challenge an affidavit by demonstrating that the affiant intentionally or recklessly omitted material information. United States v. Hoffman, 519 F.3d 672, 675 (7th Cir. 2008).

The court need not hold a Franks hearing based on conclusory or generalized assertions. See United States v. Currie, 739 F.3d 960, 963-64 (7th Cir. 2014); United States v. Taylor, 154 F.3d 675, 680 (7th Cir. 1998). Rather, the defendant must offer direct evidence of the affiant's state of mind or inferential evidence that the affiant had obvious reasons for omitting facts in order to prove deliberate falsehood or reckless disregard. United States v. Souffront, 338 F.3d 809, 822 (7th Cir. 2003). Finally, if the allegedly false statements are excluded – or the omitted facts are included – and the affidavit still supports a finding of probable cause, no hearing is required. Id.; United States v. Williams, 737 F.2d 594, 604 (7th Cir. 1984); see also Betker v. Gomez, 692 F.3d 854, 862 (7th Cir. 2012) ("We eliminate the alleged false statements, incorporate any allegedly omitted facts, and then evaluate whether the resulting 'hypothetical' affidavit would establish probable cause.").

II. THE MAGISTRATE JUDGE'S RECOMMENDATION

In the present case, the magistrate judge concluded that failing to disclose the use of the computer program, even if misleading, was not material. The affidavit still established that the government downloaded child pornography files from a computer, which agents then linked to defendant through the IP address; that the computer program may have streamlined the process of identifying the target computer did not, the magistrate judge found, upset the probable cause finding. The magistrate judge further noted that it appeared defendant actually

wanted to launch a more general attack on the constitutionality of the use of this computer program. However, defendant failed to present any evidence that the program invaded private sections of his computer, and courts have rejected constitutional challenges to law enforcement's use of forensic software, including the program used here (called "RoundUp"), to download files from P2P networks. See, e.g., United States v. Brashear, No. 4:11-CR-0062, 2013 WL 6065326, at *2-3 (M.D. Pa. Nov. 18, 2013) (collecting cases).

III. DEFENDANT'S OBJECTION

In his original objection to the recommendation, defendant argued that the agent-affiant lied, attributing the work of the computer program to an "online covert employee" (called "OCE-5023" in the warrant application), in order to conceal the government's use of RoundUp. He claimed that FBI agents regularly do this when applying for search warrants in this district. He argued that the government should bear the burden of explaining why the agent lied and of refuting his claim that the government engaged in a so-called "parallel construction" investigation.[1] He concluded that, while the agent's false statement concerning the source of his evidence did not by itself provide the basis for a Franks hearing, it did require the government to establish that the concealment of RoundUp was not an implementation of parallel construction designed to hide the acquisition of data the government had no right to

[1]In support of this claim, defendant cited an August 5, 2013 Reuters investigative report; he stated that the report revealed that "the federal government systematically instructs agents to commit perjury in affidavits to conceal the existence and work of RoundUp and thus their true sources of information and activities." (R. 36 at 2.) The report pertains to the DEA's use of intelligence intercepts to start drug investigations of Americans. Agents are apparently instructed to "recreate" the investigative trail to cover up where the information originated, a process referred to as "parallel construction." The report says nothing about RoundUp or child pornography investigations. (R. 36-1.)

examine or insert.[2]

I held a status hearing on the motion, noting that defendant's argument did not really fit under the Franks framework. It is hard to see how omitting use of this investigative technique from the affidavit undermines the facts supporting probable cause. Instead, as I advised the parties at the hearing, this seems more like a Murray/Markling argument. See United States v. Groce, 255 F. Supp. 2d 936, 943 (E.D. Wis. 2003) (citing Murray v. United States, 487 U.S. 533, 542 (1988); United States v. Markling, 7 F.3d 1309, 1315 (7th Cir. 1993)). Under those cases, a defendant may challenge a search warrant obtained based on evidence recovered during a previous, unlawful search. See United States v. Gray, 410 F.3d 338, 344 (7th Cir. 2005) ("In assessing whether the results of the subsequent search must be suppressed, we ordinarily consider whether the illegally obtained evidence affected the magistrate's decision to issue the warrant and, secondly, whether the agent's decision to obtain a warrant was prompted by knowledge of the results of the earlier illegal search."). I suggested that the parties address defendant's argument under this framework.

At the hearing, defendant presented a "proposed statement" in support of his objection. The government has filed a response, and defendant a reply. The matter is ready for decision.

---

[2]In support of his claim that agents "insert" data into suspects' computers, defendant cited articles by the computer science professors who created RoundUp discussing a process known as "tagging," pursuant to which the investigator will "tag" a remote computer over the network – inserting bit patterns into the storage media of the suspect. These tags can later be recovered from the storage media after the computer is seized pursuant to a search warrant (not unlike marked bills used in a controlled drug buy) and then used to link the remote observations to the particular suspect and his computer. In sum, the technique allows law enforcement to positively identify the seized computer as the same one that was investigated remotely. The professors indicate that this can be particularly helpful if the suspect has deleted, moved, or encrypted the material that was previously seen as available for download; tagging will also ensure that the correct machine was seized.

IV. DISCUSSION

Defendant's argument has evolved throughout the course of these proceedings. In his original objection, supporting materials, and proposed statement, defendant appeared to make two claims: (1) that the agent lied about the existence of the online covert employee (OCE-5023) in order to conceal the use of RoundUp; and (2) that RoundUp allows law enforcement to invade the private spaces of a suspect's computer. In his reply brief in support of the objection, he appears to abandon the first claim and raises a third – that RoundUp may not be sufficiently reliable. I address each of these three claims in turn.

A. Alleged False Statement

Citing other search warrant applications in this district, defendant contends that an FBI directive prevents the disclosure of RoundUp in such affidavits and requires that its use be concealed by alleging the participation of a fictitious online covert employee. In its response to the objection, the government indicates that OCE-5023 is a real person, whose name is not disclosed given his/her role in covert investigations; the government denies any deception in the warrant affidavit.

Defendant presents no evidence refuting the government's assertion; indeed, in his reply brief he appears to accept it, which dooms his request for a Franks hearing based on deception. See United States v. Johnson, 580 F.3d 666, 671 (7th Cir. 2009) (noting that the defendant must provide an evidentiary basis for a claim that the affiant lied).[5] Instead, he

[5]Defendant's claim that the agents engaged in "parallel construction" to conceal the use of RoundUp also lacks any support in the record. As noted above, the article about this tactic upon which defendant relies says nothing about RoundUp or child pornography investigations. Nor does defendant provide any legal authority for his claim that the government should be required to disprove its use of this tactic.

indicates that RoundUp may have been running unattended at the time of the downloads from his computer and argues that an evidentiary hearing is required to determine the reach of this program, how it was used in his case, and whether it is reliable.

B. Use of RoundUp to Invade Private Spaces

Relying on the articles written by RoundUp's creators, defendant contends that the program surreptitiously enters the private spaces of a target's computer and inserts data into those private spaces. I cannot find any support for that claim in the articles. The authors state: "No unauthorized access to the target's machine is required; tags are inserted in the normal function of a system." (R. 38-2 at 6.)[6] The authors also suggest that the hash value of the tag be provided to the magistrate as part of the search warrant application (id.), which controverts defendant's claim that agents using the program are instructed to conceal their activities. The articles provide no non-speculative basis for believing that RoundUp may be used to invade private spaces. Nor do the articles discuss tagging in relation to the "Ares" P2P network, which was used in the present case. Based on materials defendant previously submitted, it appears that RoundUp for Ares was developed by the Ontario Provincial Police, rather than the computer science professors who wrote the articles upon which defendant now relies. (See R. 27-2 at 2.) In any event, even if RoundUp could be used improperly, defendant makes no claim that the government invaded the private spaces of his computer, to insert tags or to

[6]In an article previously submitted by defendant, the RoundUp creators stated that the "software does not allow law officers to hack into an individual's private computer. . . . It simply provides law enforcement with an 'optimized interface for observation' which allows an investigator to watch the open activities of remote peers on the network." (R. 27-4 at 1.)

search for evidence, despite the fact that he had forensic experts examine the computer.[7] He admits that he does not know whether tagging was even being used at the time his computer was accessed.[8]

Defendant asks for a hearing so the court can determine whether agents used the program to enter the unshared space on his computer, but the district court is required to hold a hearing on a motion to suppress only if the defendant's allegations are sufficiently definite, specific, non-conjectural, and detailed. United States v. Curlin, 638 F.3d 562, 564 (7th Cir. 2011). Given the speculative nature of defendant's claims, there is no need to hold a hearing and no basis for concluding that illegally obtained evidence was used to obtain the warrant, as in the Murray/Markling line of cases. See, e.g., United States v. Stults, 575 F.3d 834, 842-44 (8th Cir. 2009) (denying motion to suppress evidence gathered pursuant to a search warrant based on downloads from a P2P file-sharing network).

C. Reliability of RoundUp

In his reply brief, defendant notes that, according to the search warrant affidavit, OCE-5023 downloaded files from defendant's computer between 2:11 a.m. and 3:33 a.m. on November 25, 2012. Defendant presents an affidavit from his computer expert, who indicates

---

[7]The government further indicates that it provided in the discovery materials investigative logs that detailed the online operation.

[8]Defendant contends that, according to the designers, one of the problems with RoundUp is the "unacceptable incidence of false positives," which the designers solved through tagging. (R. 39 at 3.) However, in the paper defendant filed, the authors "define false positives as when a machine that was never tagged appears to be tagged." (R. 38-2 at 7.) The paper does not support defendant's apparent claim that RoundUp erroneously identifies computers as containing child pornography when they really don't. Defendant makes no claim of a false positive in his case, and the government indicates that remnants of the files the agent remotely downloaded were later found during a forensic examination of defendant's computer.

that the agent-affiant admitted to him that the computer program was running unattended during the time of the downloads. (R. 42-2 at 2.) Defendant argues that the failure to disclose this information prevented the magistrate judge from evaluating the reliability of the acquisition process. In support of this new claim, he cites another article, which generally discusses issues with the reliability of computer software.

Even assuming that the program was running unattended at the time of the downloads, defendant provides no authority in support of his claim that this precludes a finding of probable cause. Nor does he claim that the FBI failed to confirm that the material downloaded was, in fact, child pornography. The warrant affidavit includes a detailed description of three of the files. (R. 23-2 at 15-16 ¶ 27.) This is not a situation where a computer program downloaded material believed to be contraband (based on, say, a keyword search or hash values) and no human being looked at the material before a warrant was sought. The affidavit further indicates that, after the images were downloaded and confirmed to be child pornography, the FBI identified the IP address from which the images were downloaded and, pursuant to a subpoena to the internet service provider, identified defendant as the subscriber. This process is sufficiently reliable to support the issuance of the warrant.[9] See, e.g., United States v. Craighead, 539 F.3d 1073, 1080-81 (9th Cir. 2008); United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007).

Finally, I decline to hold an evidentiary hearing to explore the reliability and capabilities of RoundUp. Hearings on motions to suppress are not granted as a matter of course. United

[9]The article attached to the reply brief does not discuss RoundUp or the use of such software to obtain search warrants. Rather, it primarily discusses the reliability of computer-generated evidence at trial. It thus provides no support for defendant's claim.

States v. Villegas, 388 F.3d 317, 324 (7th Cir. 2004). District courts are required to conduct evidentiary hearings only when a substantial claim is presented, there are disputed issues of material fact that will affect the outcome of the motion, and the defendant's allegations are sufficiently specific and non-conjectural. Curlin, 638 F.3d at 564. Here, defendant offers only speculation about RoundUp. Accordingly, there is no basis for holding a hearing.

V. CONCLUSION

THEREFORE, IT IS ORDERED that the magistrate judge's recommendation (R. 33) is adopted, and defendant's motion to suppress (R. 21, 22, 24) is **DENIED**.

IT IS FURTHER ORDERED that this matter is scheduled for **STATUS** on **Friday, March 21, 2014, at 11:30 a.m.**

Dated at Milwaukee, Wisconsin, this 17th day of March, 2014.

/s Lynn Adelman

_____

LYNN ADELMAN
District Judge